Name - Krish Sharma

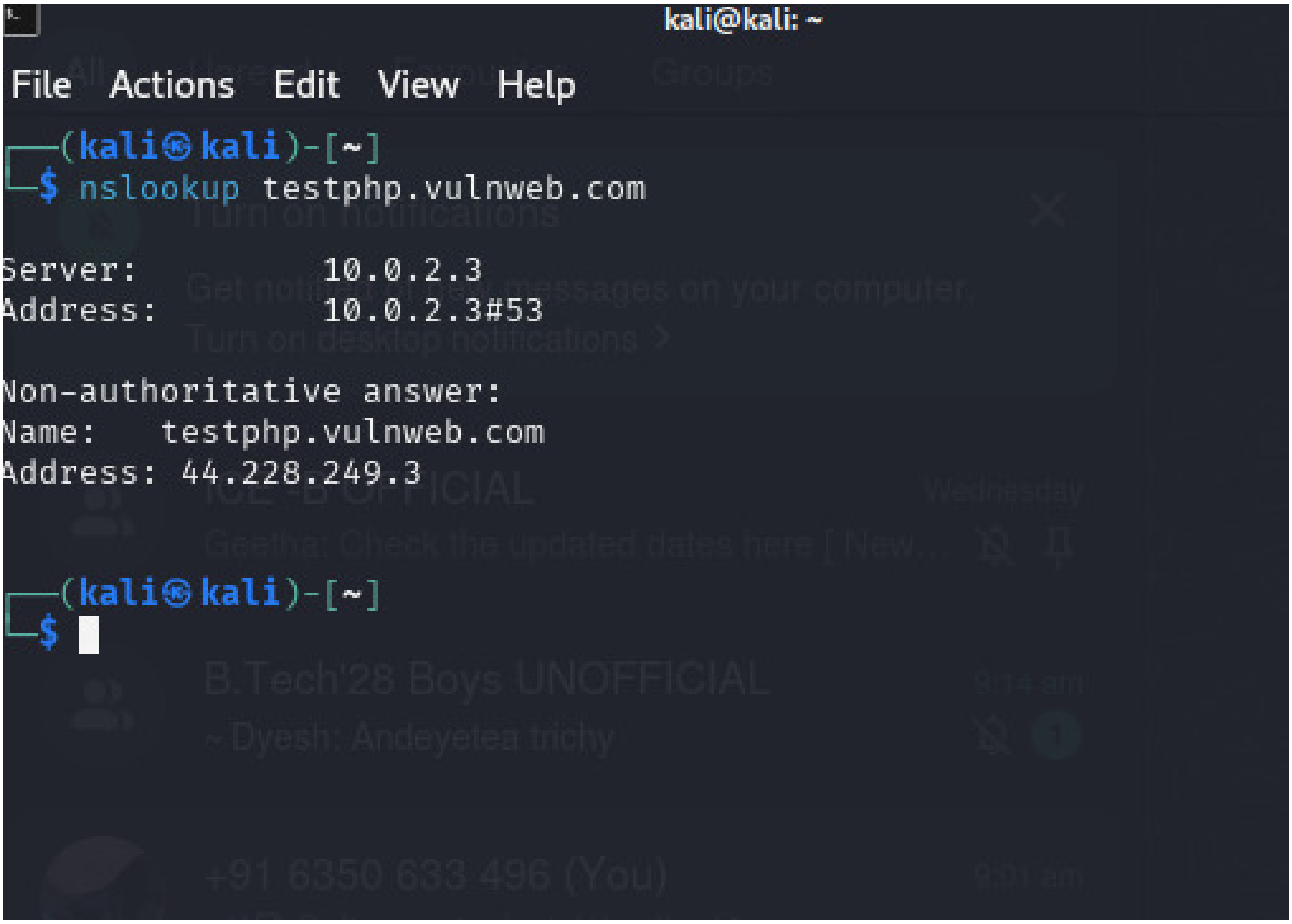
Roll No - 110124062

Spider task submission (domain specific)

Web security Level 1

Performing Recon on http://testphp.vulnweb.com

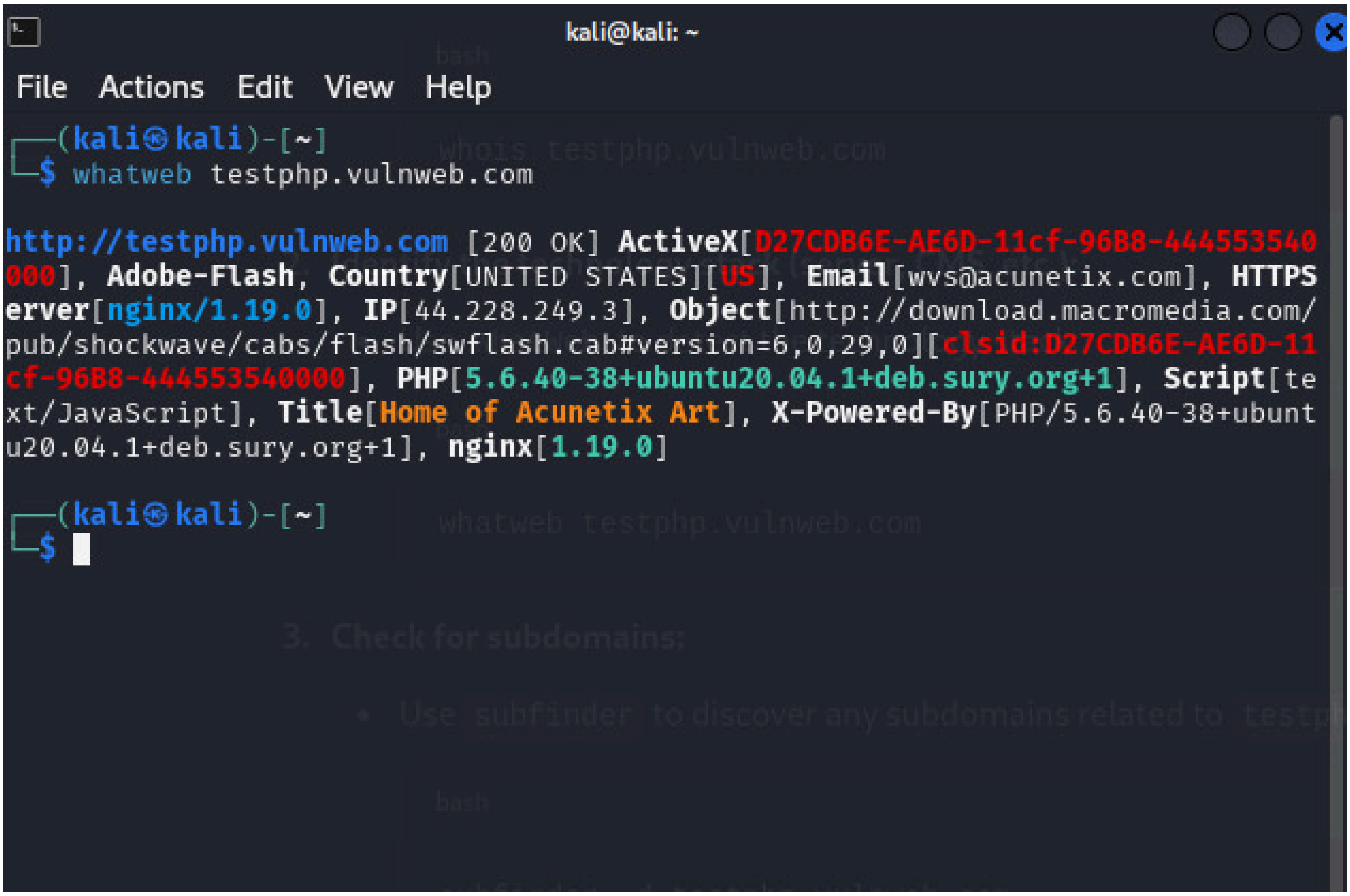
Passive recon -



```
┌──(kali㉿kali)-[~]
└─$ nslookup testphp.vulnweb.com

Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
Name:   testphp.vulnweb.com
Address: 44.228.249.3


┌──(kali㉿kali)-[~]
└─$ 
```

tool used - nslookup

ip address - 44.228.249.3



```
┌──(kali㉿kali)-[~]
└─$ whatweb testphp.vulnweb.com

http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540
000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.com], HTTPS
erver[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/
pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:D27CDB6E-AE6D-11
cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[te
xt/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubunt
u20.04.1+deb.sury.org+1], nginx[1.19.0]

┌──(kali㉿kali)-[~]
└─$ 
```

tool used - whatweb

used for - additional DNS info

HTTP Status: [200 OK] – This indicates that the server is responding correctly with a successful HTTP status code.

ActiveX: [D27CDB6E-AE6D-11cf-96B8-444553540000] – This is the identifier for an ActiveX control, which could be a security concern depending on the application.

Adobe Flash – Indicates the web application uses Flash, which is now deprecated and should be avoided due to security risks.

Country: [UNITED STATES][US] – The server is located in the United States.

Email: wvs@acunetix.com – This could be a contact email associated with the application, likely related to security or vulnerability testing (Acunetix is a security testing tool).

HTTP Server: nginx/1.19.0 – The web server is running nginx version 1.19.0.

IP: 44.228.249.3 – This is the IP address of the server (which you already identified earlier).

Object:
http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0 – A reference to an ActiveX Flash object (which is outdated and not secure).

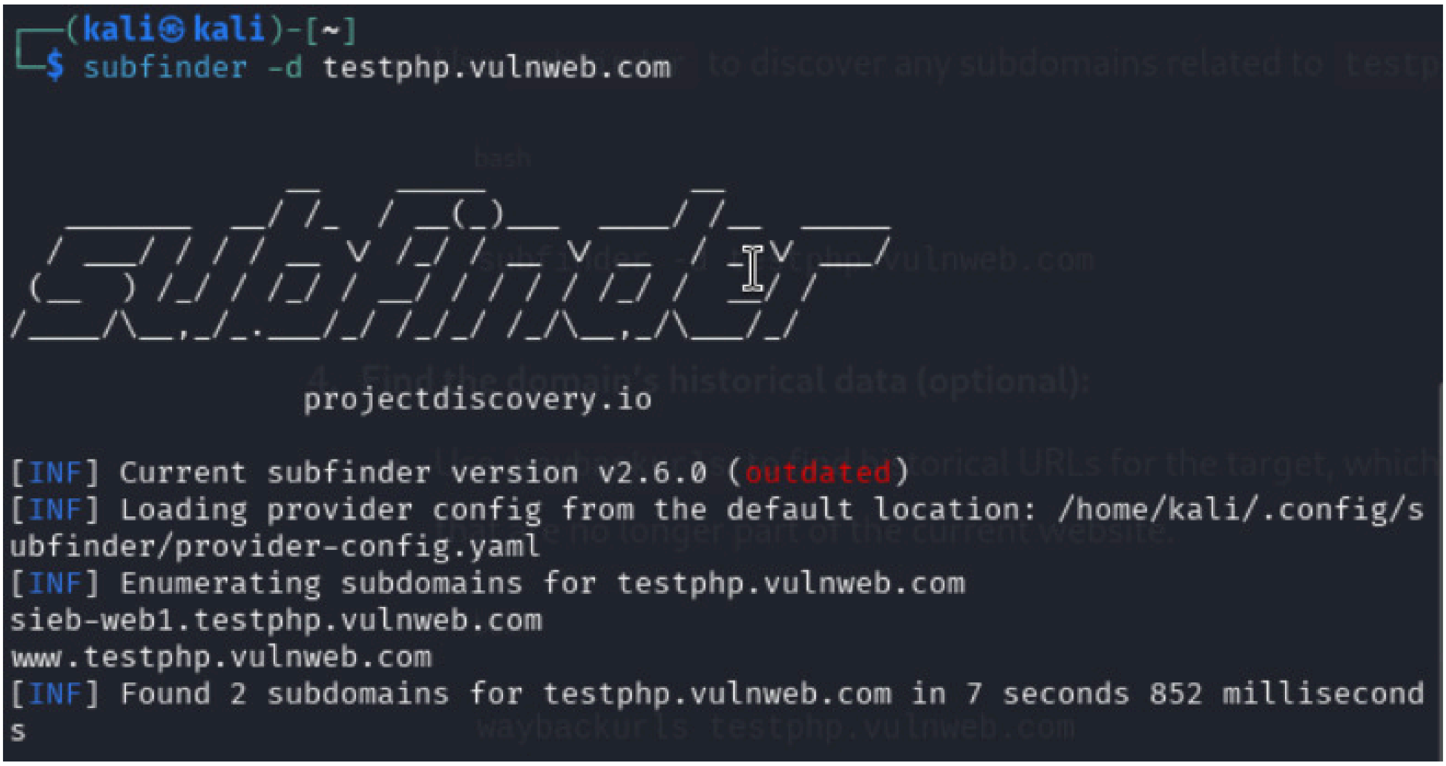
PHP Version: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 – The web server is running PHP version 5.6.40. This version is outdated and could have security vulnerabilities.

Script Type: text/JavaScript – The website uses JavaScript for client-side scripting.

Title: Home of Acunetix Art – The title of the page is "Home of Acunetix Art," which may relate to a security or vulnerability testing platform.

X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 – This header reveals the PHP version again, potentially giving insight into the server's technology.

nginx: 1.19.0 – Confirms again that the server is running nginx version 1.19.0.



```
┌──(kali㉿kali)-[~]
└─$ subfinder -d testphp.vulnweb.com


               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from the default location: /home/kali/.config/s
ubfinder/provider-config.yaml
[INF] Enumerating subdomains for testphp.vulnweb.com
sieb-web1.testphp.vulnweb.com
www.testphp.vulnweb.com
[INF] Found 2 subdomains for testphp.vulnweb.com in 7 seconds 852 millisecond
s
```

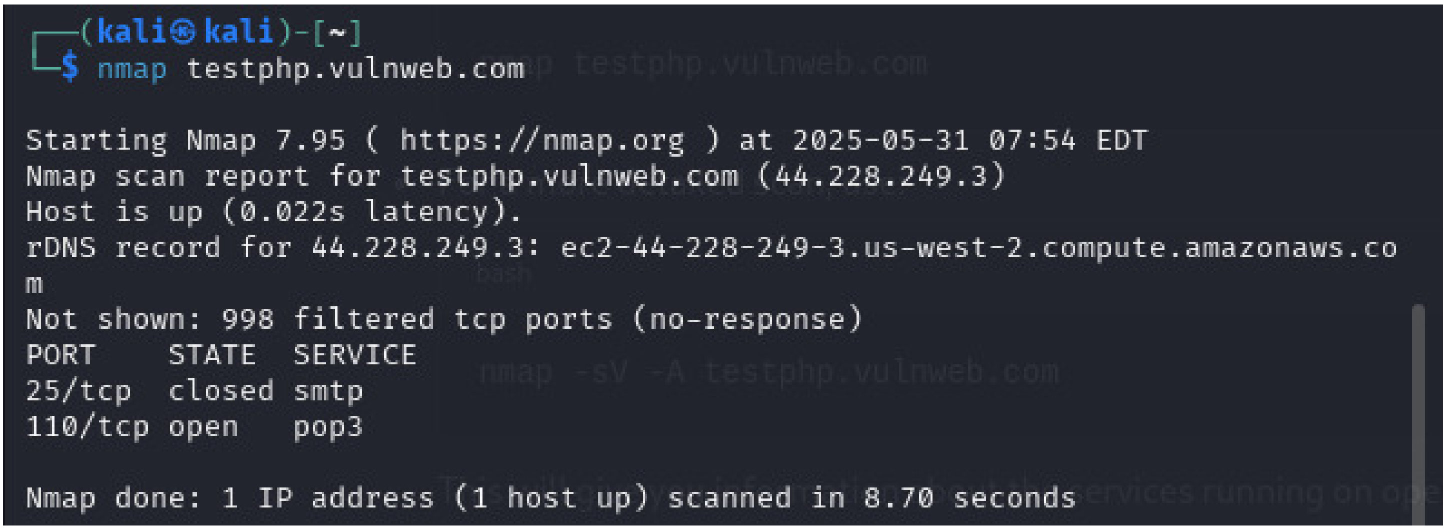
tool used - subfinder

for finding subdomains

sieb-web1.testphp.vulnweb.com

www.testphp.vulneb.com

Active recon -



```
┌──(kali㉿kali)-[~]
└─$ nmap testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 07:54 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.022s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE  SERVICE
25/tcp  closed smtp
110/tcp open   pop3

Nmap done: 1 IP address (1 host up) scanned in 8.70 seconds
```

tool used - nmap

for finding open ports and services

Host Information:

The host is up and responsive with a low latency of 0.022s.

Reverse DNS (rDNS) record: The server is hosted on AWS (ec2-44-228-249-3.us-west-2.compute.amazonaws.com).

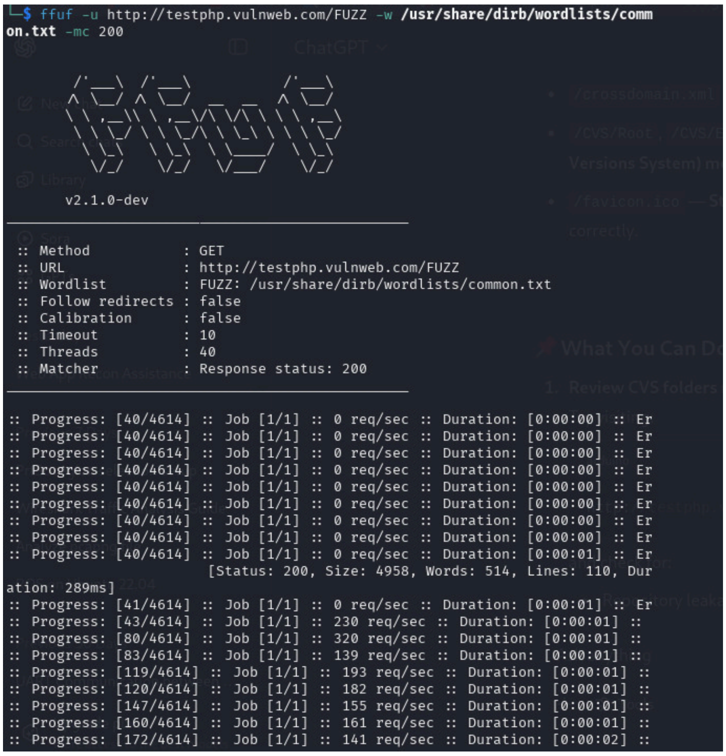
Ports:

Port 25/tcp: Closed – This port is typically used for SMTP (Simple Mail Transfer Protocol), which is often used for email services. Since it's closed, the server is not accepting connections on this port.

Port 110/tcp: Open – This port is used for POP3 (Post Office Protocol 3), which is used to retrieve email from a mail server. Since it's open, it suggests that the server may have an email service running on this port.

Filtered Ports:

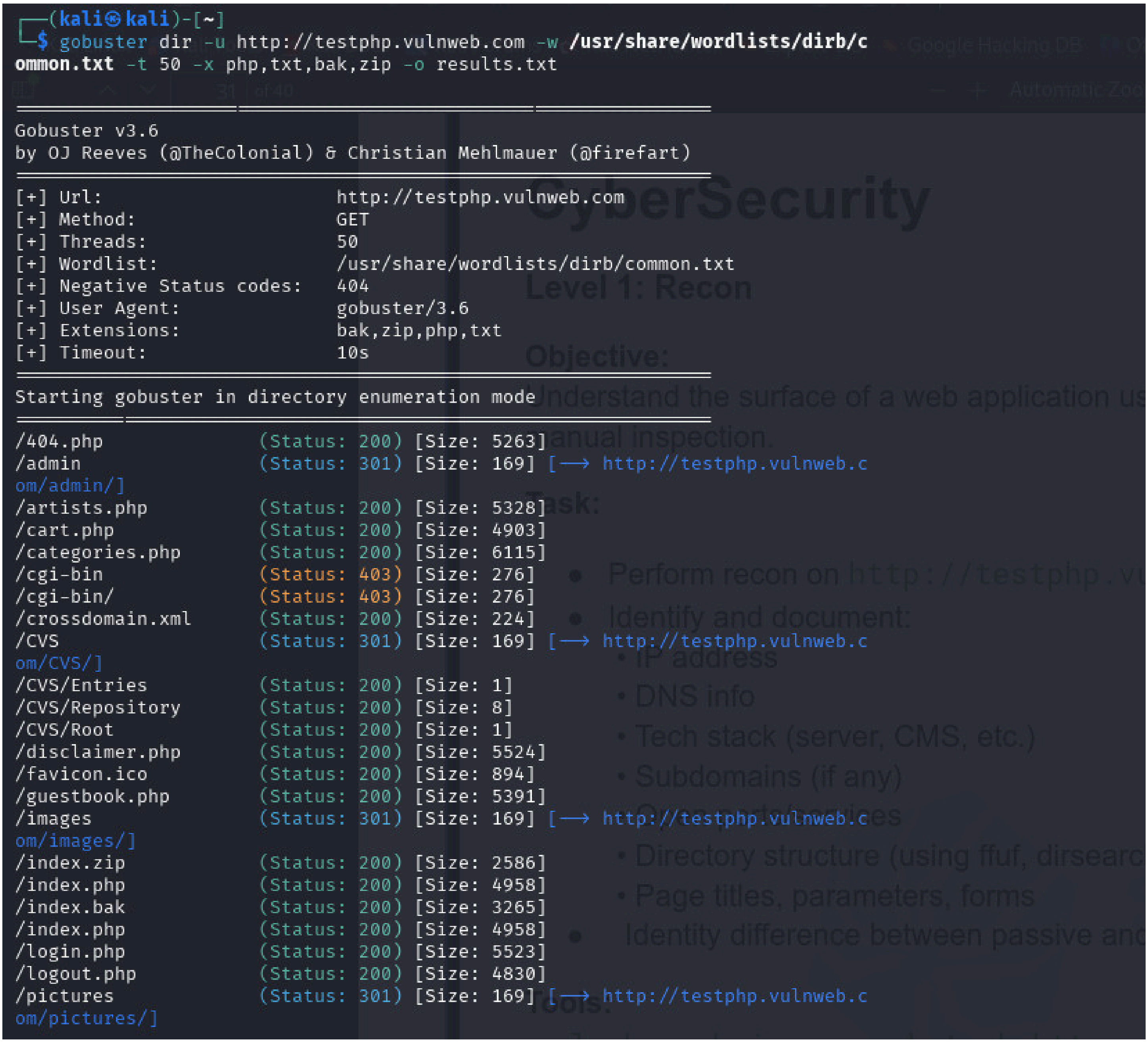
998 filtered TCP ports – These ports are not shown because they are either blocked by a firewall or do not respond. These could be ports associated with different services or protocols.



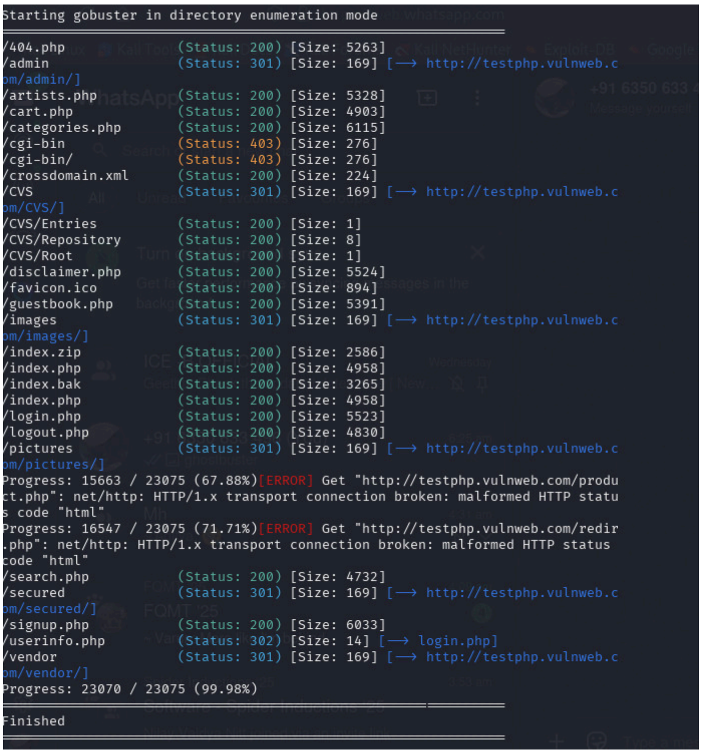
```
└─$ ffuf -u http://testphp.vulnweb.com/FUZZ -w /usr/share/dirb/wordlists/comm
on.txt -mc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://testphp.vulnweb.com/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200
________________________________________________

:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Er
:: Progress: [40/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:01] :: Er
                        [Status: 200, Size: 4958, Words: 514, Lines: 110, Dur
ation: 289ms]
:: Progress: [41/4614] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:01] :: Er
:: Progress: [43/4614] :: Job [1/1] :: 230 req/sec :: Duration: [0:00:01] ::
:: Progress: [80/4614] :: Job [1/1] :: 320 req/sec :: Duration: [0:00:01] ::
:: Progress: [83/4614] :: Job [1/1] :: 139 req/sec :: Duration: [0:00:01] ::
:: Progress: [119/4614] :: Job [1/1] :: 193 req/sec :: Duration: [0:00:01] ::
:: Progress: [120/4614] :: Job [1/1] :: 182 req/sec :: Duration: [0:00:01] ::
:: Progress: [147/4614] :: Job [1/1] :: 155 req/sec :: Duration: [0:00:01] ::
:: Progress: [160/4614] :: Job [1/1] :: 161 req/sec :: Duration: [0:00:01] ::
:: Progress: [172/4614] :: Job [1/1] :: 141 req/sec :: Duration: [0:00:02] ::
```

tool used - ffuf , to find directories

/crossdomain.xml /CVS/Root, /CVS/Entries, /CVS/Repository/favicon.ico , these directories returned 200 OK status i.e. they exist



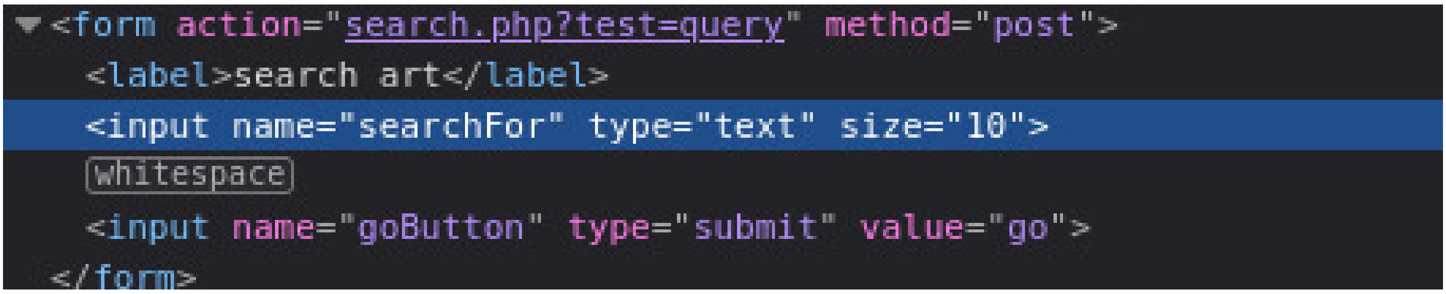
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/c
ommon.txt -t 50 -x php,txt,bak,zip -o results.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              bak,zip,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/404.php              (Status: 200) [Size: 5263]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/admin/]
/artists.php          (Status: 200) [Size: 5328]
/cart.php             (Status: 200) [Size: 4903]
/categories.php       (Status: 200) [Size: 6115]
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin/             (Status: 403) [Size: 276]
/crossdomain.xml      (Status: 200) [Size: 224]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/CVS/]
/CVS/Entries          (Status: 200) [Size: 1]
/CVS/Repository       (Status: 200) [Size: 8]
/CVS/Root             (Status: 200) [Size: 1]
/disclaimer.php       (Status: 200) [Size: 5524]
/favicon.ico          (Status: 200) [Size: 894]
/guestbook.php        (Status: 200) [Size: 5391]
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/images/]
/index.zip            (Status: 200) [Size: 2586]
/index.php            (Status: 200) [Size: 4958]
/index.bak            (Status: 200) [Size: 3265]
/index.php            (Status: 200) [Size: 4958]
/login.php            (Status: 200) [Size: 5523]
/logout.php           (Status: 200) [Size: 4830]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/pictures/]
```



```
Starting gobuster in directory enumeration mode
===============================================================
/404.php              (Status: 200) [Size: 5263]
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/admin/]
/artists.php          (Status: 200) [Size: 5328]
/cart.php             (Status: 200) [Size: 4903]
/categories.php       (Status: 200) [Size: 6115]
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin/             (Status: 403) [Size: 276]
/crossdomain.xml      (Status: 200) [Size: 224]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/CVS/]
/CVS/Entries          (Status: 200) [Size: 1]
/CVS/Repository       (Status: 200) [Size: 8]
/CVS/Root             (Status: 200) [Size: 1]
/disclaimer.php       (Status: 200) [Size: 5524]
/favicon.ico          (Status: 200) [Size: 894]
/guestbook.php        (Status: 200) [Size: 5391]
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/images/]
/index.zip            (Status: 200) [Size: 2586]
/index.php            (Status: 200) [Size: 4958]
/index.bak            (Status: 200) [Size: 3265]
/index.php            (Status: 200) [Size: 4958]
/login.php            (Status: 200) [Size: 5523]
/logout.php           (Status: 200) [Size: 4830]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/pictures/]
Progress: 15663 / 23075 (67.88%)[ERROR] Get "http://testphp.vulnweb.com/produ
ct.php": net/http: HTTP/1.x transport connection broken: malformed HTTP statu
s code "html"
Progress: 16547 / 23075 (71.71%)[ERROR] Get "http://testphp.vulnweb.com/redir
.php": net/http: HTTP/1.x transport connection broken: malformed HTTP status
code "html"
/search.php           (Status: 200) [Size: 4732]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/secured/]
/signup.php           (Status: 200) [Size: 6033]
/userinfo.php         (Status: 302) [Size: 14] [--> login.php]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.c
om/vendor/]
Progress: 23070 / 23075 (99.98%)
===============================================================
Finished
===============================================================
```

tool used - ghostbuster , to find hidden directories

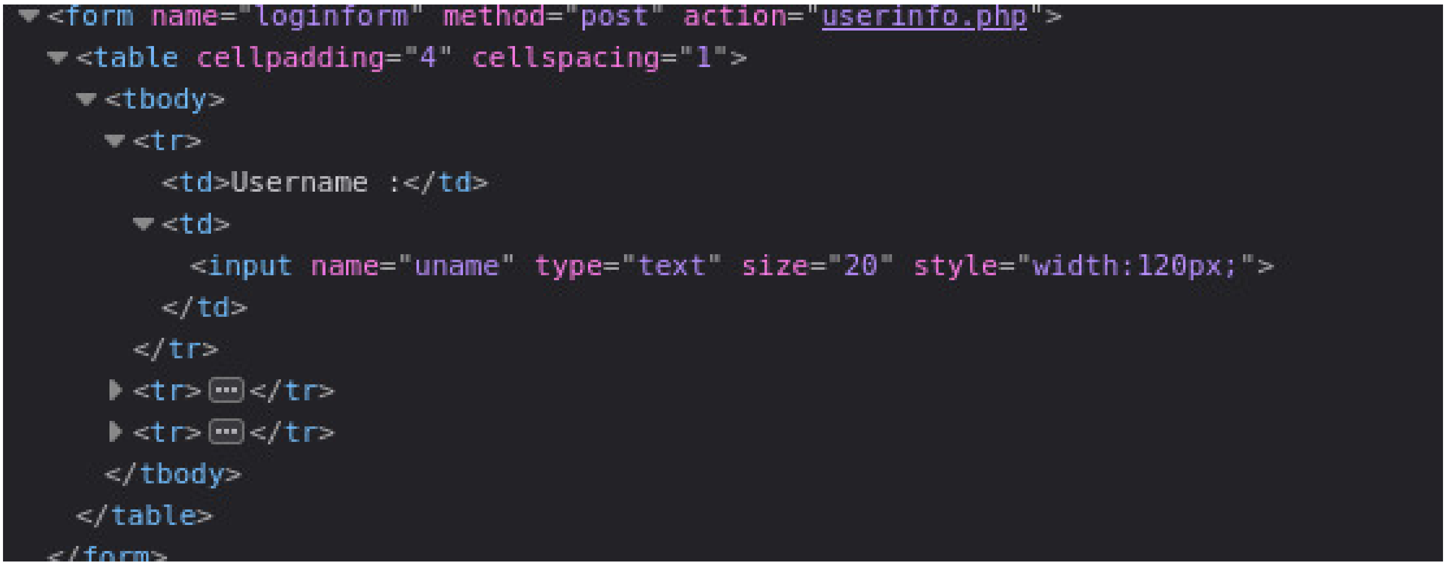
forms and parameters found -



```
▼<form action="search.php?test=query" method="post">
   <label>search art</label>
   <input name="searchFor" type="text" size="10">
   whitespace
   <input name="goButton" type="submit" value="go">
 </form>
```

search bar on site (form)

parameter - input



```
▼<form name="loginform" method="post" action="userinfo.php">
  ▼<table cellpadding="4" cellspacing="1">
    ▼<tbody>
      ▼<tr>
          <td>Username :</td>
        ▼<td>
            <input name="uname" type="text" size="20" style="width:120px;">
          </td>
        </tr>
      ▶<tr>…</tr>
      ▶<tr>…</tr>
      </tbody>
    </table>
  </form>
```

login form , parameter - input